

## **REMARKS**

Claims 1-39 were pending and presented for examination and were pending in this application. In an Office Action dated February 25, 2008, claims 1-39 were rejected. No claims are amended herein. No new claims have been added. Reconsideration and allowance of claims 1-39 is respectfully requested.

### **Response to Rejection Under 35 USC 103(a)**

Claims 1-19 and 21-36, 38 and 39 were rejected as allegedly being obvious under 35 USC § 103(a) in view of U.S. Patent No. 6,137,782 to Sharon et al. (“Sharon”) and U.S. Patent No. 6,754,181 to Elliot (“Elliot”)<sup>1</sup>. This rejection is respectfully traversed.

Claim 1 recites:

A network application monitoring system, comprising:

- (a) at least one media module coupled to an associated network segment on which the network application is running, each media module for monitoring and collecting data relating to traffic on the associated network segment corresponding to the network application and for analyzing, responsive to a trigger condition, the collected data for traffic information, wherein each media module is tailored for network analysis and is configurable to a monitoring mode or a focus mode to monitor and collect data; and
- (b) an application server module coupled to the at least one media module for receiving the collected data and the analyzed data and analyzing the collected data and the analyzed data for improving the performance of the network application, for configuring the trigger condition, for transmitting the trigger condition to the at least one media module, the application server module associating a user with the collected data and the analyzed data and generating a user specific log file including the collected data, the analyzed data and the associated user.

Hence, the media module monitors network traffic and collects and analyzes data from the collected network responsive to a trigger condition. The trigger condition produces

---

<sup>1</sup> Although the summary of the rejection merely references claims 1-19 and 21-36, the rejection addresses claims 1-19, 21-36 and claims 38 and 39.

actions in response to specified events. The application server module configures the trigger condition, associates data from the media module with a user and generates a user-specific log file including the data from the media module. Hence, the claimed invention beneficially allows storage of data from the media module in a user-specific log file which includes network traffic data associated with an individual user. This user-specific log file simplifies analysis and/or monitoring of different users' network traffic by including data from the media module. Therefore, the application server module beneficially allows configuration of the trigger conditions used to receive data from the media module and allows user-specific monitoring and analysis of network application use.

In contrast, Sharon discloses an agent 14 which at most examines received frames and examines the source and destination address to determine whether a source or destination address is unknown (Sharon, col. 7, lines 7-15). The agent receives a command from a central management engine (CME) 12 to either begin collecting and transmitting data or stop data transmission and collection (Sharon, col. 7, lines 41-55). The CME 12 uses the collected data to determine placement of network agents within a network traffic topology map (Sharon, col. 3, lines 26-41). Hence, the CME 12 receives network data and analyzes the traffic flow between different network elements for correction and modification of traffic flow through a network topology (Sharon, col. 3, lines 45-46; col. 5, lines 26-29).

The CME 12 merely determines a frequency of packet flow between network elements and switches the agents 14 between a mode where they eavesdrop on network traffic and a mode where they do not eavesdrop on network traffic (Sharon, col. 4, lines 14-18; col. 6, lines 45-54). There is no disclosure in Sharon that the CME 12 associates "a user

with the collected data and the analyzed data” or generates “a user specific log file including the collected data, the analyzed data and the associated user.” The CME 12 does not associate received data with a user, but merely correlates received data with different time slots (Sharon, col. 8, lines 60-66). Hence, the CME 12 allows for association of data with different time slots, but does not associate received data with a user or generate a log file including data associated with the user (Sharon, col. 8, line 66-col. 9, line 3).

Unlike the temporal classification of the CME 12, the application server module of the claimed invention generates a user-specific log file, which associates received data with a particular user. This user-specific log file allows network traffic to be categorized or analyzed according to the user associated with the data, simplifying analysis of how different users impact network traffic. In contrast, the CME 12 merely monitors network traffic based on data source and destination then categorizes the monitored data into time slots regardless of a network user. As the Examiner admits in the Final Office Action, there is no disclosure in Sharon of an application server module “associating a user with the collected data and the analyzed data and generating a user specific log file including the collected data, the analyzed data and the associated user,” as claimed.

Elliott fails to remedy the deficient disclosure of Sharon. Rather, Elliott merely discloses a hybrid network which uses telephony routing information and internet protocol address information to transfer information across the internet (Elliott, col. 1, lines 27-33). However, Elliott fails to disclose an application server module “associating a user with the collected data and the analyzed data and generating a user specific log file including the collected data, the analyzed data and the associated user,” as claimed. While Elliott discloses a user interface including a user’s application profile, this profile does not associate “a user

with the collected data and the analyzed data” or generate “a user specific log file including the collected data, the analyzed data and the associated user,” as claimed (Elliott, col. 63, lines 4-9). Elliott describes a user account profile which merely summarizes account information for different services such as “directlineMCI profile, Information Services profile, Global Message Handling, List Management and Personal Home Page profiles.” Hence, the user profile only describes the features and functionality which a user can access through the network. Rather than associate a user with analyzed data, Elliott only discloses a list of services available to an individual user (Elliott, col. 64, lines 1-9).

Elliott also consolidates messages to a user in a centralized information store, where a user can review his or her messages but these messages are not analyzed and the analyzed messages also associated with the user (Elliott, col. 64, lines 11-25). While the claimed invention associates both analyzed data and collected data with a user, Elliott merely maintains a record of different services or functions and messages that can be accessed by a specific user account. Rather than allow for user-specific analysis of network traffic, Elliott only uses a profile to identify different services or data accessible by various users.

Although Elliott also discloses a monitoring function for capturing data-related events and statistical measurements, the captured data is not associated with a user, as claimed. In Elliott, various metrics are captured and subsequently analyzed to identify overall system performance or monitor for specific thresholds, but these metrics are never associated with a user or used to generate a user specific log file (Elliott, col. 37, lines 41-47). Although Elliott logs captured data, the log is not user specific as the captured data is never associated with an individual user transmitting or receiving the data, but merely describes overall network performance or characteristics. At most, Elliott determines whether a packet belongs to a

special group of packets to determine packet priority, but this determination is based on characteristics of the packet itself, regardless of which user transmits the packet (Elliott, col. 19, lines 60-65). Hence, while the claimed user specific log file enables analysis of network resource consumption by various users, Elliott merely allows for evaluation of overall network resource consumption by multiple users. Therefore, Elliott does not disclose an application server module “associating a user with the collected data and the analyzed data” and “generating a user specific log file including the collected data, the analyzed data and the associated user” as claimed.

Therefore, for at least the reasons described above, claim 1 is patentably distinguishable over Sharon and Elliott, both alone and in combination.

As claims 2-19 and 21 are dependent from claim 1, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 2-19 and 21. Therefore, claims 2-19 and 21 are also patentably distinct from Sharon and Elliott, both alone and in combination.

Independent claims 22 and 23 similarly recite “associating a user with analyzed received data and the analyzed data” and “generating a user specific log file including the analyzed received data and the associated user.” Claims 24-36 and 38 depend from claim 23 which, as amended, now recites similar limitations to claim 1. Therefore, the arguments advanced above with respect to claim 1 are also applicable to claims 24-36 and 38. Hence, claims 24-36 and 38 are also patentably distinct from Sharon and Elliott, both alone and in combination.

Independent claim 39 similarly recites “the application server module associating a user with the collected data and the analyzed data and generating a user specific log file

including the collected data, the analyzed data and the associated user,” so the arguments advanced above with respect to claim 1 are also applicable to claim 39. Hence, claim 39 is also patentably distinct from Sharon and Elliott, both alone and in combination.

To establish *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. See MPEP §2143.03. The deficient disclosures of Sharon and Elliott preclude establishing a *prima facie* basis from which a proper determination of obviousness of claims 1-19, 21-36, 38 and 39 can be made. Therefore, it is respectfully submitted that claims 1-19, 21-36, 38 and 39 are patentably distinct from Sharon and Elliott, both alone and in combination.

Claims 20 and 37 were rejected as allegedly being obvious under 35 USC § 103(a) in view of Sharon and U.S. Patent No. 6,681,232 to Sistanizadeh et al. (“Sistanizadeh”). This rejection is respectfully traversed.

Claim 20 is dependent from claim 1. As explained above, Sharon does not disclose an application server module “associating a user with the collected data and the analyzed data and generating a user specific log file including the collected data, the analyzed data and the associated user” as recited in amended claim 1. Similarly, claim 37 is dependent from claim 23, which recites “associating a user with analyzed received data and the analyzed data” or “generating a user specific log file including the analyzed received data and the associated user.” As explained above, Sharon fails to disclose “associating a user with the collected data and the analyzed data and generating a user specific log file including the collected data, the analyzed data and the associated user,” “associating a user with analyzed received data and the analyzed data” or “generating a user specific log file including the analyzed received data and the associated user,” as claimed.

Sistanizadeh has been cited for including graphs and logs as part of reports based on the monitored data. However, Sistanizadeh discloses a service level manager allowing users to obtain service through a network and providing report options about user network service (Sistanizadeh, col. 20, line 65 to col. 21, line 14). The service level manager in Sistanizadeh provides a user interface and network topology for improving network operation support, but Sistanizadeh fails to disclose or suggest an application server module “associating a user with the collected data and the analyzed data and generating a user specific log file including the collected data, the analyzed data and the associated user,” as claimed. Thus, Sistanizadeh fails to remedy the deficient disclosure of Sharon as the references, both alone and in combination, do not disclose or suggest the application server module of the claimed invention.

To establish *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. See MPEP §2143.03. The deficient disclosures of Sharon and Sistanizadeh preclude establishing a *prima facie* basis from which a proper determination of obviousness of claims 20 and 37 can be made. Therefore, it is respectfully submitted that claims 20 and 37 are patentably distinct from Sharon and Sistanizadeh, both alone and in combination.

### **Conclusion**

In sum, it is respectfully submitted that claims 1-39, as presented herein, are patentably distinguishable over the cited references (including references cited, but not applied) and are in condition for allowance. Favorable action is solicited.

Respectfully Submitted,  
MIKE MORAN, ET AL

Date: April 25, 2008

By: /Brian G. Brannon/

Brian G. Brannon, Attorney of Record  
Registration No. 57,219  
FENWICK & WEST LLP  
801 California Street  
Mountain View, CA 94041  
Phone: (650) 335-7610  
Fax: (650) 938-5200